

# NONVOLATILE MEMORY DEVICE

**Publication number:** JP11232884 (A)

**Publication date:** 1999-08-27

**Inventor(s):** TAKEUCHI MIKI; TANIGAWA HIROYUKI +

**Applicant(s):** HITACHI LTD +

**Classification:**

- **international:** **G06F12/14; G06F21/24; G11C16/02; G06F12/14; G06F21/00; G11C16/02; (IPC1-7): G11C16/02; G06F12/14**

- **European:**

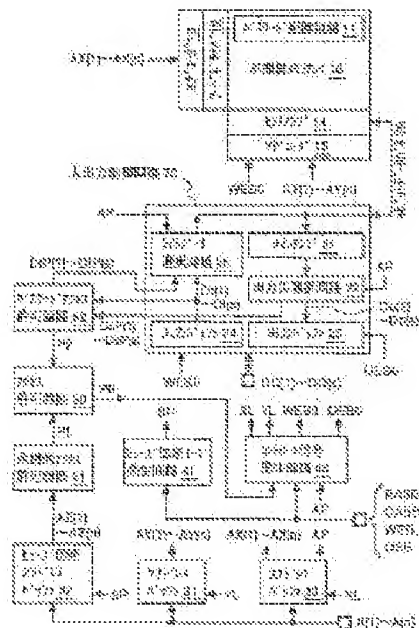
**Application number:** JP19980027471 19980209

**Priority number(s):** JP19980027471 19980209

## Abstract of JP 11232884 (A)

**PROBLEM TO BE SOLVED:** To provide a device having an access limit and which releases the limit only for a prescribed user by utilizing a password stored in a part of plural memory cells for releasing the access limit in a first access permission means and utilizing none of information stored in plural memory cells in a second access permission means.

**SOLUTION:** A password access permission circuit 52 uses the passwords DoP(1)-DoP(s) stored in a password storage area 11 of a nonvolatile memory array 10 and internal write-in signals Di(1)-Di(s) answering to the data DQ(1)-DQ (s) imparted from the outside generated in an input buffer 24 to make signal P2 high level and generates the information DiP(1)-DiP(s) to be rewritten. An X address buffer 30 latches address signals A(1)-A(n) from the outside by a timing signal XL to generate X address signals AX(1)-AX(s).



.....  
Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-232884

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 1 1 C 16/02

G 1 1 C 17/00

6 0 1 P

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 C

審査請求 未請求 請求項の数18 O L (全 15 頁)

(21) 出願番号 特願平10-27471

(22) 出願日 平成10年(1998) 2月9日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 竹内 幹

東京都小平市上水本町五丁目20番1号 株

式会社日立製作所半導体事業部内

(72) 発明者 谷川 博之

東京都小平市上水本町五丁目20番1号 株

式会社日立製作所半導体事業部内

(74) 代理人 弁理士 玉村 静世

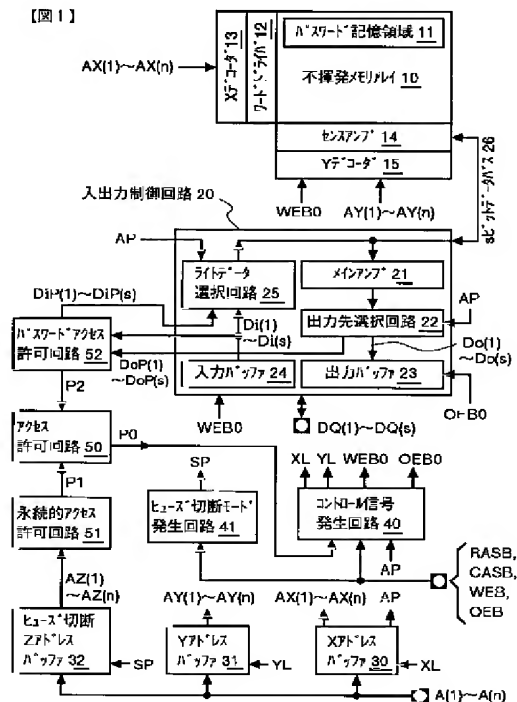
(54) 【発明の名称】 不揮発性メモリ装置

(57) 【要約】

【課題】 アクセス制限機能を有し、特定のユーザのみが該制限を解除できる不揮発性メモリ装置を提供する。

【解決手段】 不揮発性メモリ装置の記憶領域の一部に格納されたパスワードを活用した第1のアクセス許可手段と、該記憶領域のいかなる情報も活用しない第2のアクセス許可手段を設ける。上記記憶領域の一部に格納された情報に基づいて、ライトまたはリードまたはその両方を禁止するアクセス制限のうちひとつを選択する手段を設ける。上記パスワードの一部の情報に基づいて、読み出された上記パスワードを自動消去するか、あるいは再書き込みするかを選択する、再書き込み選択手段を設ける。パスワード情報がリテンション不良等により失われてもアクセス制限を解除できる。簡単な付加回路で、高信頼のセキュリティ機能が実現できる。

【図1】



**【特許請求の範囲】**

【請求項1】 電気信号で書き換え可能な複数の不揮発のメモリセルと、該複数のメモリセルの情報を外部とやりとりするための制御回路とが設けられ、該制御回路は、上記複数のメモリセルの少なくとも一部に対してリードまたはライトまたはその両方を禁止するアクセス制限手段と、該アクセス制限を解除する第1のアクセス許可手段と、上記アクセス制限を解除する第2のアクセス許可手段とを少なくとも備え、該第1のアクセス許可手段は、アクセス制限を解除するにあたって、上記複数のメモリセルの一部に格納されたパスワードを活用し、上記第2のアクセス許可手段は、上記複数のメモリセルに格納された情報を一切活用しないことを特徴とする不揮発性メモリ装置。

【請求項2】 上記第2のアクセス許可手段は、一回限り書き込み可能な複数の記憶素子を活用し、該複数の記憶素子の記憶状態の組み合わせが取りうる複数の状態のうち、所定の一つの状態に記憶素子を設定した場合にアクセス制限を解除するものであることを特徴とする請求項1記載の不揮発性メモリ装置。

【請求項3】 上記第2のアクセス許可手段は、アクセス制限解除のための動作をただ一回に限る手段をさらに含んでいることを特徴とする請求項2記載の不揮発性メモリ装置。

【請求項4】 上記第2のアクセス許可手段は、ユーザに開放されていない制御方法によってアクセス制限の解除が行なわれるものであることを特徴とする請求項1記載の不揮発性メモリ装置。

【請求項5】 電気信号で書き換え可能な複数の不揮発のメモリセルと、該複数のメモリセルの情報を外部とやりとりするための制御回路とが設けられ、該制御回路は、上記複数のメモリセルの少なくとも一部に対して、電源投入直後にはリード及びライトアクセス両方を禁止し、その後上記複数のメモリセルの一部に格納された第一の情報に基づいてリードまたはライトまたはその両方を禁止するアクセス制限のうちひとつを選択して設定する手段と、該選択設定手段に関与する上記第一の情報の書換えを許可し、該アクセス制限を解除する第1のアクセス許可手段とを少なくとも備え、該第1のアクセス許可手段による上記書換え許可及びアクセス制限解除は、上記複数のメモリセルの一部に格納されたパスワードと外部から与えられる情報との関係に基づいて決定されるものであることを特徴とする不揮発性メモリ装置。

【請求項6】 上記第1のアクセス許可手段は、上記外部から与えられる情報が、上記パスワードに一致した場合に、上記書換え許可及びアクセス制限解除を行うものであることを特徴とする請求項5記載の不揮発性メモリ装置。

【請求項7】 上記第1のアクセス許可手段は、上記外部から与えられる情報が上記パスワードに一致しない場

合、上記パスワードの格納に割り当てられているメモリセルに所定の値を書き戻すようにされ、上記読み出されたパスワードが上記所定の値である場合には、上記書換え許可及びアクセス制限の解除を行なわないものであることを特徴とする請求項6記載の不揮発性メモリ装置。

【請求項8】 上記複数のメモリセルは、強誘電体キャパシタと電界効果トランジスタを有してなるものであることを特徴とする請求項5記載の不揮発性メモリ装置。

【請求項9】 上記第1のアクセス許可手段は、ダイナミック ランダム アクセス メモリにおけるリード モディファイ ライト コマンドと同じ制御信号手順を与えることにより実行され、この際に外部から与えられるライトデータと上記パスワードとの比較により上記書換え許可及びアクセス制限解除を行うものであることを特徴とする請求項5記載の不揮発性メモリ装置。

【請求項10】 上記パスワードは複数組格納可能であることを特徴とする請求項5記載の不揮発性メモリ装置。

【請求項11】 電気信号で書き換え可能な複数の不揮発のメモリセルと、該複数のメモリセルの情報を外部とやりとりするための制御回路とが設けられ、該制御回路は、上記複数のメモリセルの少なくとも一部に対してリードまたはライトまたはその両方を禁止するアクセス制限手段と、該アクセス制限を解除する第1のアクセス許可手段とを少なくとも備え、該第1のアクセス許可手段によるアクセス制限の解除は、上記複数のメモリセルの一部に書き込まれたパスワードと外部から与えられる情報との関係に基づいて決定され、さらに上記第1のアクセス許可手段は、上記アクセス制限の解除を行なわないことを決定した場合、常に所定の値を書き戻すか、あるいは常に読み出されたパスワードを再書き込みするかの何れかを選択して行うパスワード再書き込み手段を有し、該パスワード再書き込み手段による上記選択は、上記複数のメモリセルの一部に書き込まれた情報に基づいて決定されることを特徴とする不揮発性メモリ装置。

【請求項12】 上記第1のアクセス許可手段は、上記外部から与えられる情報が、上記パスワードに一致した場合に、上記アクセス制限の解除を行うものであることを特徴とする請求項11記載の不揮発性メモリ装置。

【請求項13】 上記パスワード再書き込み手段による上記選択は、上記読み出されたパスワードの一部の情報を活用して行なわれるものであることを特徴とする請求項11記載の不揮発性メモリ装置。

【請求項14】 上記複数のメモリセルは、強誘電体キャパシタと電界効果トランジスタを有してなる者であることを特徴とする請求項11記載の不揮発性メモリ装置。

【請求項15】 上記第1のアクセス許可手段は、ダイナミック ランダム アクセス メモリにおけるリード モディファイ ライト コマンドと同じ制御信号手順を与えることにより実行され、この際に外部から与えられるラ

イトデータと上記パスワードとの比較によりアクセス制限の解除を行うものであることを特徴とする請求項1記載の不揮発性メモリ装置。

【請求項16】 上記パスワードは複数組格納可能であることを特徴とする請求項1記載の不揮発性メモリ装置。

【請求項17】 上記第1のアクセス許可手段は、誤った手順のために該第1のアクセス許可手段によるアクセス制限解除に失敗した場合、電源を再投入しなければ、次に正しい手順で第1のアクセス許可手段によるアクセス制限解除を再試行してもアクセス制限解除は行なわれないようにする再試行防止手段を含み、該再試行防止手段は、安定な第1又は第2の状態を有し、電源投入直後には第1の状態にあり、一旦第1の状態から第2の状態に移した後は、電源を再投入しない限り二度と第1の状態に復帰できない回路を含んで成るものであることを特徴とする請求項1記載の不揮発性メモリ装置。

【請求項18】 電気信号で書き換え可能な複数の不揮発のメモリセルと、該複数のメモリセルの情報を外部とやりとりするための制御回路とが設けられ、該制御回路は、上記複数のメモリセルの少なくとも一部に対してリードまたはライトまたはその両方を禁止するアクセス制限手段と、該アクセス制限を解除する第1のアクセス許可手段とを少なくとも備え、該第1のアクセス許可手段によるアクセス制限の解除は、上記複数のメモリセルの一部に書き込まれたパスワードと外部から与えられる情報との関係に基づいて決定され、さらに上記第1のアクセス許可手段は、上記パスワードをメモリセルから読出した後、読み出されたパスワードの一部の情報を規則的に変更して書き戻すか、或いは読み出されたパスワードをそのまま書き込みするか何れかを選択して行うパスワード再書き込み手段を有し、該パスワード再書き込み手段による上記選択は、上記複数のメモリセルの一部に書き込まれた情報と外部から与えられる情報との関係に基づいて決定されるものであることを特徴とする不揮発性メモリ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アクセス制限機能を有する不揮発性メモリチップ又は同チップを内蔵したICメモリカード等の不揮発性メモリ装置に関するものである。

【0002】

【従来の技術】近年の情報化社会において、ICメモリカードに格納した情報を機密に保持したい（リードアクセスを制限したい）、あるいは不正に書き換えられることを防止したい（ライトアクセスを制限したい）という要求は大きい。

【0003】こうしたアクセス制限機能を実現するために考えられる単純な方法は、メモリカードに搭載したRO

Mにパスワードを保持しておき、このパスワードと一致した入力をメモリカードに与えた場合にアクセスを許可するようにすることである。しかしながら、不正アクセスを試みるものは、種々のパスワードを試行することができるので、高い機密性は保証されない。

【0004】さらに高度なアクセス制限を実現するために、よく知られた暗号技術を応用することが考えられる。すなわち、暗号化キーを保持したROMと、該キーを用いて任意の平文を暗号文に変換する演算装置とからなる暗号化装置をICメモリカードに設ける。メモリカードにアクセスする場合、任意の平文とこれに対応する暗号文とがデジタル信号としてメモリカードに与えられる。与えられた暗号文がメモリカード内部で計算された暗号文に一致した場合、メモリカードのアクセス制限が解除される。このメモリカードに対しては、暗号化キーと暗号変換方式とを知るものだけがアクセスできる。

【0005】

【発明が解決しようとする課題】しかしながら、上記暗号化方式を汎用のICメモリカードに適用する場合、以下のような問題がある。

【0006】（1）上記暗号化装置が故障すると、メモリカードへのアクセスがまったく不能になる。たとえば、リードアクセス制限を行っていた場合、メモリカードへは重要なデータが格納されていることが多いので、上記暗号化装置の故障は重大な障害となる。

【0007】（2）上記暗号化装置を設けることにより、ICメモリカードを構成するチップの面積が増大しコストの上昇を招く。あるいは、搭載メモリの大容量化が阻害される。

【0008】（3）メモリカードに平文と暗号文とを与えるにあたり、暗号文を生成するための第2の暗号化装置が別途必要となる。第2の暗号化装置の機密管理が必要である。

【0009】（4）一旦暗号化キーが第三者に知られると、ROMに格納された暗号化キーを変更することはできないので、もはやアクセス制限機能は完全に失われる。

【0010】（5）メモリカードが第三者に盗み出された場合、第三者は十分な時間をかけて試行錯誤によりアクセス制限の解除に成功する可能性がある。

【0011】（6）第三者が試行錯誤によりアクセス制限の解除に成功しても、その痕跡が全く残らない。したがって、リードアクセス制限を行っていた場合、情報の漏えいが認識できない。ライトアクセス制限を行っていた場合、第三者が不正な書き換えを行っても、これを認識できない。

【0012】なお、アクセス制御機能をソフトウェアにより実現する方法も考えられるが、ICメモリカードはいかなる装置に装着して用いられるかわからないので、ソフトウェアにより実現する方法は危険である。

【0013】本発明の目的は、アクセス制限機能をも

し、特定のユーザのみが該制限を解除できる不揮発性メモリ装置または不揮発ICメモリカードを提供する。

【0014】本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかなるであろう。

【0015】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。

【0016】すなわち、本発明の不揮発性メモリ装置は、アクセス制限を解除する第1のアクセス許可手段と、第2のアクセス許可手段とを有する。上記第1のアクセス許可手段は、アクセス制限を解除するにあたって、本発明の書換可能な不揮発性メモリ装置の一部のメモリセルに書き込まれたパスワードを活用する。アクセス制限は、ライトまたはリードまたはその両方に対して設定される。

【0017】第2のアクセス許可手段は、第1のアクセス許可手段においてメモリセルに書き込んだパスワードがリテンション不良等により失われたり、ユーザが自分の設定したパスワードを忘れたりした場合に備えて設けられる。

【0018】本発明の一つの形態においては、上記第2のアクセス許可手段は、一回限り書き込み可能な複数の記憶素子（たとえばヒューズ）を有する。第2のアクセス許可手段は、該複数の記憶素子の記憶状態の組み合わせが取りうる複数の状態のうち、アクセス制限解除を指定する一つの状態に記憶素子を設定する。さらに、本発明の一つの形態においては、第2のアクセス許可手段の使用をただ一回に制限するための回路をさらに設けることができる。

【0019】上記第2のアクセス許可手段は、本発明のメモリ装置が通常用いられる環境とは異なる環境、たとえば通常より高い電源電圧のもとで動作され、或いは、特殊なコマンドにより動作されるように、実現することができる。これにより、誤動作防止を促進できる。

【0020】さらに、本発明の一つの形態においては、上記第1のアクセス許可手段に用いられる該パスワードをメモリセルから読出した後には、常に所定の値（たとえば0）が書き戻され、上記第1のアクセス許可手段は、該書き戻しが完了した後にアクセス制限を解除する内部信号を発生できるように構成される。そして、読み出されたパスワードが該所定の値である場合には、アクセス制限を解除する内部信号が発生しないように第1のアクセス許可手段は構成される。さらに、その一つの形態においては、本発明の不揮発性メモリ装置は強誘電体メモリであり、上記第1のアクセス許可手段は、ダイナミック ランダム アクセス メモリ（DRAM）におけるリード モディファイ ライト コマンドと同じ制御信号手順を与えることにより実行される。

【0021】本発明の一つの形態においては、上記第1のアクセス許可手段に用いられる該パスワードをメモリセルから読出した後には、常に所定の値（たとえば0）が書き戻されるか、あるいは常に読み出されたパスワードが書き込みされるかの何れかが行なわれる。何れの書き戻しを行うかの選択は、本発明の不揮発性メモリ装置のメモリセルに書き込まれた情報に基づいて決定することができる。好ましくは、該情報は上記読み出されたパスワードの一部に割り当てられている。

【0022】本発明の一つの形態においては、上記第1のアクセス許可手段によるアクセス制限解除に一度失敗した場合、電源を再投入しなければ、次に正しい手順で第1のアクセス許可手段を再試行してもアクセス制限解除は行なわれないようにする再試行防止手段を含んでいる。該再試行防止手段は、2つの安定な状態を有し、電源投入直後には第1の状態にあり、一旦第1の状態から第2の状態に遷移した後は、電源を再投入しない限り二度と第1の状態に復帰できない回路を含んでいる。

【0023】本発明の一つの形態においては、アクセス制限を、ライトまたはリードまたはその両方から選択設定する権利を限られたユーザにのみ与える手段を有している。その手段による選択は、本発明の不揮発性メモリ装置のメモリセルに書き込まれた情報を基に決定することができる。

【0024】

【発明の実施の形態】以下に本発明の不揮発性メモリ装置の具体的な例を示すが、該メモリ装置はメモリチップの形態であっても、ICカードの形態であっても良い。また、以下では、1996年電子情報通信学会英文誌C分冊E79-C巻の第234から242頁（IEICE Transactions on Electronics, vol.E79-C, no.2, pp.234-242, 1996）に示されている「強誘電体キャパシタを有するVcc/2プレートの不揮発性DRAM」に適用した場合、すなわちDRAMと同様な制御が可能な不揮発性メモリを想定して例を示すが、他の形態の不揮発性メモリに対しても、本発明の本質が適用できることは言うまでもない。強誘電体キャパシタを有するVcc/2プレートの不揮発性DRAMは、特に図示はしないが、メモリセルとして、例えば、選択トランジスタとしての電界効果トランジスタと、これに直列接続された強誘電体キャパシタとを有して構成される。選択トランジスタのゲート電極がワード線に、ソース（又はドレイン）がビット線に接続される。

【0025】《不揮発性メモリ装置の全体的な一例》図1には本発明に係る不揮発性メモリ装置の第1の例がブロック図で示される。内部データバス26はsビットの幅（ビット数）を持っており、一つのXアドレスおよびYアドレスの指定に従って、sビットのデータがやりとりされる。

【0026】不揮発性メモリ装置において、リードアクセスを制限する場合、アクセス許可回路50の出力P0が

ロウレベルの時にはコントロール信号発生回路40で生成されるメモリ内部のアウトプット イネーブル バー信号OEB0は常にハイレベル（出力ネゲート状態）となり、メモリセルアレイ10の読出しデータは信号DQ(1)～DQ(s)として外部に出力されない。

【0027】ライトアクセスを制限する場合、出力P0がロウレベルの時にはコントロール信号発生回路40で生成されるメモリ内部のライト イネーブル バー信号WEB0は常にハイレベル（書き込みネゲート状態）となり、外部からの信号DQ(1)～DQ(s)はメモリセルアレイ10に書き込まれない。

【0028】上記出力P0は、永続的アクセス許可回路51からの信号P1と、パスワードアクセス許可信号52からの信号P2の何れかがハイレベルとなった場合にハイレベルとなり、アクセス制限を解除する。

【0029】まず永続的アクセス許可手段について説明する。たとえば、永続的アクセス許可回路51は、複数のヒューズを有し、これらのヒューズのうちある特定の複数のヒューズが切断された場合にのみ、信号P1をハイレベルとする。切断するヒューズの選択は、ヒューズ切断 Zアドレスバッファ32からの出力AZ(1)～AZ(n)により行なわれる。Zアドレスバッファ32はタイミング信号SPにより外部からのアドレス信号A(1)～A(n)をラッチし、AZ(1)～AZ(n)として出力する。SPは、外部から制御信号RASB、CASB、WEB、OEBが特定の手順で与えられた場合に、ヒューズ切断モード発生回路41において生成される。以上のように、永続的アクセス許可手段はヒューズの組み合わせで実現されるので、一旦信号P1がハイレベルになるとその状態が保たれる。また、不適当なヒューズを切断すると、二度と信号P1をハイレベルにできない。尚、前記制御信号RASB、CASB、WEB、OEBは、DRAMの一般的なアクセス制御信号である、ロウアドレスストロブ、カラムアドレスストロブ、ライトイネーブル、アウトプットイネーブルの各信号と同一機能の信号と理解されたい。

【0030】次にパスワードアクセス許可手段について説明する。パスワードアクセス許可回路52は、メモリセルアレイ10のパスワード記憶領域11に格納されたパスワードDoP(1)～DoP(s)と、外部から与えられるデータDQ(1)～DQ(s)に対応して入力バッファ24で発生する内部書き込み信号Di(1)～Di(s)とを用いて、信号P2をハイレベルとする。もっとも単純な例ではDoP(1)～DoP(s)とDi(1)～Di(s)とが一致した場合に信号P2をハイレベルとする。さらに回路52は、パスワード記憶領域11に再書き込みすべき情報DiP(1)～DiP(s)を発生する。特に制限されないが、P2が一旦ハイレベルにされると、メモリの動作電源が投入されている限り、P2の状態はそのまま維持される。

【0031】上記のパスワードアクセス許可手段において、DoP(1)～DoP(s)は次の手順で回路52に与えられ

る。すなわち、まずXアドレスバッファ30はタイミング信号XLにより外部からのアドレス信号A(1)～A(n)をラッチし、Xアドレス信号AX(1)～AX(n)を発生する。ここで、A(1)～A(n)を記憶領域11のXアドレスに一致させておくと、パスワードアクセスフラグAPがハイレベルとなり、記憶領域11へのアクセスであることを示す。APがハイレベルの場合、コントロール信号発生回路40は、外部からのWEB、OEBに一致して内部信号WEB0、OEB0を発生し、アクセス制限を行わない。制限を行わないでもパスワードの漏えいやパスワードの勝手な書き換えが不可能であることは、後述の説明で明かとなる。

【0032】Xアドレス発生に引き続き、Yアドレスバッファ31はタイミング信号YLにより外部からのアドレス信号A(1)～A(n)をラッチし、Yアドレス信号AY(1)～AY(n)を発生する。ここで、AX(1)～AX(n)、AY(1)～AY(n)により記憶領域11内の所望のパスワードが選択されるようにA(1)～A(n)を与える。なお、AX(1)～AX(n)が記憶領域11を示し、AY(1)～AY(n)が記憶領域11に格納された複数のパスワードのうち一つを選択するように構成できる。すなわち、異なるパスワードを複数個保持できる。上記信号XL、YLは、外部から制御信号RASB、CASB、WEB、OEBが特定の手順で与えられた場合に、コントロール信号発生回路40において生成される。これは、DRAMにおける公知の信号発生手段と等しい。

【0033】上記アドレス指定において、WEBをハイレベルに設定しておく、内部信号WEB0もハイレベルとなり読出し動作が行なわれる。すなわち、Xデコーダ13、ワードドライバ12を経て、記憶領域11のワード線が活性化され、記憶領域11のデータはセンスアンプ14にラッチされる。Yデコーダ15により所望のパスワードDoP(1)～DoP(s)が選択され、sビット幅のデータバス16を経て入出力制御回路20へ送られる。そこでパスワードDoP(1)～DoP(s)はメインアンプ21にラッチされる。出力先選択回路22はAPがハイレベルであることに対応してDoP(1)～DoP(s)をパスワードアクセス許可回路52へ送る。なお、出力先選択回路22はAPがロウレベルの場合のみメモリセルアレイ10からの読出しデータを出力バッファ23へ送るようになっており、記憶領域11のデータが外部へ読み出されないようにしている。すなわちパスワードの漏えいを防いでいる。以上が、DoP(1)～DoP(s)が回路52に到達するまでの手順である。

【0034】上記のパスワードアクセス許可手段において、回路52で生成されたDiP(1)～DiP(s)は次のようにして記憶領域11に再書き込みされる。すなわち、ライトデータ選択回路25は、APがハイレベルの場合DiP(1)～DiP(s)を、APがロウレベルの場合Di(1)～Di(s)をライトデータとして選択する。記憶領域11が選択されていた場合、APはハイレベルであり、DiP(1)～DiP(s)はデータバス26、センスアンプ14を経て、記憶領域11に

再書き込みされる。なお、選択回路25の上記機能により、先に述べたように記憶領域11に対してはライト制限を受けないように構成しているにもかかわらず、外部信号DQ(1)~DQ(s)により生成されるDi(1)~Di(s)が直接記憶領域11に書き込まれないようにしている。すなわち、パスワードが勝手に書き換えられないようになっている。

【0035】以上、本発明の主要な構成要素である回路50、51、52の働きについて説明した。信号P0がハイレベルとなり、アクセス制限が解かれた後には、通常のメモリとして動作するのでここでは詳述しない。本発明の主要な構成要素のより具体的な回路の例は後述される。

【0036】図1に示した不揮発性メモリ装置によれば、以下の効果が得られる。

【0037】(1)通常使用されるパスワードアクセス許可手段が故障しても、あるいは記憶領域11のパスワードがなんらかの障害、たとえば不揮発性メモリセルのリテンション不良やハードエラー、ユーザの設定パスワード忘却などにより失われても、永続的アクセス許可回路51によりアクセス制限回路を解除できるので、高信頼のセキュリティ機能が得られる。

【0038】(2)パスワードを書換可能な不揮発性メモリセルに格納するので、たとえば一回ごとにこれを変更することにより、入力パスワードとの直接比較による単純なアクセス制限解除方式を採用できる。ただし、この場合、後の例に示すように、内部パスワードと入力パスワードの不一致時には、内部パスワードを自動消去するなど、試行錯誤による不正アクセスを防止する施策が施される。このような単純なアクセス制限解除方式の採用によりチップ面積が低減でき、その結果コストを下げられる。あるいは、本メモリ使用時に第2の暗号化装置が別途必要になることもない。したがって、特に汎用メモリチップおよび汎用ICカードに適したセキュリティ機能付き不揮発メモリが得られる。

【0039】(3)パスワードを書換可能な不揮発性メモリセルに格納するので、パスワードを第三者に知られてもこれを変更することにより引き続きメモリのセキュリティを維持することができる。

【0040】(4)上記(2)で述べたような不正アクセス時の内部パスワード消去を行えば、単純な構成で極めてセキュリティの高いメモリが得られるが、パスワードアクセス許可回路52によるアクセス制限解除が不能となる。これに備えて、永続的アクセス許可回路51の存在、あるいはその詳細な方法を限られた機関、たとえばICカードメーカーのみの機密としておけば、アクセス制限の解除が可能である。特に、後の具体例に示すように、永続的アクセス許可回路51を通常の使用条件の範囲外に設定しておけば、この存在を知らないユーザが意図せず該手段を行使する危険を回避でき、極めてセキュ

リティが高く、かつアクセス制限解除が不能となる危険性も小さい汎用のメモリが得られる。

【0041】(5)上記(2)で述べたような不正アクセス時の内部パスワード消去を行えば、ユーザはパスワードアクセス手段が不能となったことにより不正アクセスが試みられたかも知れないと察知できる。これによりユーザはセキュリティ態勢をより強化するなどの対策をとることができる。

【0042】《永続的アクセス許可手段の具体例》以下図2~図7により、永続的アクセス許可手段の具体的な構成例を示す。

【0043】図2は、永続的アクセス許可回路51の一構成例を示すものである。回路51は、アドレス信号AZ(i)とAZ(m+1)、AZ(m+2)を入力とし、ヒューズ状態信号FS(i)を出力とするヒューズ状態信号発生回路511-i(i=1~m)と、FS(i)を入力としP1を出力とするヒューズ状態論理回路512とからなる。

【0044】回路511-iの具体的回路例が図3に示されている。回路511-iは、ヒューズF(i)が接続状態の時出力FS(i)をロウレベルに、切断状態の時高抵抗R(i)の働きによりFS(i)をハイレベルにする。ヒューズ切断はAZ(m+1)、AZ(m+2)が共にハイレベルのとき可能となる。この時アドレス信号AZ(i)がハイレベルであれば、F(i)に大電流が流れ切断される。なお、F(i)の切断は電源電圧Vccが通常使用条件より高くなければ行なわれないように、ヒューズを設計しておけば、実施例1の効果(4)で述べた効果が得られる。ヒューズ素子自体は、DRAMの冗長回路などで公知の技術である。

【0045】回路512の具体的回路例が図4に示されている。F(i)(i=1~m)のハイレベル/ロウレベルの組み合わせがある一つの状態の場合に限り、信号P1がハイレベルとなる。該状態は、アンド素子へのFS(i)入力の前段にインバータが設けられているか否かにより一に決定される。信号P1をハイレベルとして、アクセス制限を解除するためには、論理回路512の構成にしたがってアドレス信号AZ(1)~AZ(m)を正しく入力することが要求される。

【0046】図5はヒューズ切断モード発生回路41の具体的な回路例である。レジスタ412はS入力(セット入力)がロウレベルからハイレベルに遷移したときにQ出力(非反転出力)をハイレベルとし、R入力(リセット入力)がロウレベルからハイレベルに遷移したときにQ出力をロウレベルにする。回路411はCASP、WEBがハイレベルからロウレベルに遷移してからT1<Tp<T2の範囲にある時間TpにRASBがハイレベルからロウレベルに遷移した場合、SPsetをロウレベルからハイレベルに遷移させる。ここで、T1は遅延回路411の遅延要素delay(411)により定まり、T2は遅延要素delay(412)により定まる。また、RASBがハイレベルからロウレベルに遷移した場合、遅延要素delay(414)で定まる幅のパルスが発生



する。回路411はさらに、RASBがロウレベルからハイレベルに遷移した場合、遅延要素delay(413)で定められるパルス幅のリセットパルスを発生する。以上の構成により、回路41は、CASB、WEBがハイレベルからロウレベルに遷移してから $T1 < T_p < T2$ の範囲にある時間 $T_p$ にRASBがハイレベルからロウレベルに遷移するとSPをハイレベルとし、RASBがロウレベルからハイレベルに戻るとSPをロウレベルに戻す。

【0047】図6は、図5の回路41とZアドレスバッファ32とによるヒューズ切断アドレスAZ(1)~AZ(n)の生成を示すタイミング図である。図5で述べたようにしてRASB、CASB、WEB遷移に対応してSPがハイレベルに遷移すると、回路32は外部からのアドレス信号A(1)~A(n)をラッチしAZ(1)~AZ(n)を出力する。SPがハイレベルの間AZ(1)~AZ(n)は出力され続けられるが、RASBがハイレベルとなり、この結果SPがロウレベルになると、AZ(1)~AZ(n)はすべて0にリセットされる。

【0048】以上図2から図6に示した構成により、回路512で一意に定められるヒューズを切断した後は永続的にアクセス制限が解除される。本実施例の永続的アクセス許可手段においては、(1)通常より高い電源電圧を必要とすること、(2)特殊なRASB、CASB、WEBの与え方をすること、(3)RASBをロウレベルに遷移させるタイミングが $T1 < T_p < T2$ に制約されていることにより、通常の使用条件で本手段が行使される偶発的事故は極めてまれと考えられる。あるいは仮に不正アクセスを試みるものが永続的アクセス解除手段の存在と上記

(1)と(2)の事実を知ったとしても、上記(3)が、誤ったヒューズの切断及びその結果としてのアクセス制限解除不能という事態を回避する。すなわち、パスワードアクセス許可回路52が不能になったときのバックアップ手段として、上記永続的アクセス許可回路51は高いデータ保護機能を実現するものである。

【0049】図7はヒューズ切断モード発生回路41の別の回路例を示すものである。図5の構成では、不正アクセスを試みるものは数回に渡りヒューズ切断の試行を重ねることができる。たとえば、前記ヒューズ状態論理回路512で定められる状態が、全てのヒューズを切断という状態だった場合、F(1)からF(m)まで順にヒューズ切断を試み、一回ごとにアクセス制限解除に成功したか調べる方法を取られた場合、最終的に不正なアクセス制限解除に成功する。図7は回路41の起動を一回のみに制限し、不正アクセスの排除をより完全に行う回路である。図7ではこの目的のため、回路413が設けられる。回路413の構成は図3の回路511-iと同様である。SP、AZ(m+1)、AZ(m+2)がすべてハイレベルとなり、AZ(1)~AZ(m)に従ったヒューズ切断が開始されると、アンド素子の出力により回路413のヒューズF(SP)も切断される。この結果、回路413の出力FS(SP)がハイレベルとなり、レジスタ412のS入力にハイレベルが与

えられることは二度とない。すなわち、SPは二度とハイレベルにならず、したがってAZ(1)~AZ(n)を二度と発生できない。本発明の実施例により、不正なアクセス制限解除に成功する確率を下げることができる。

【0050】《パスワードアクセス許可手段の具体例》以下図8~図13により、パスワードアクセス許可手段の具体的な構成例を示す。

【0051】図8は、パスワードアクセス許可回路52の構成例を示すものである。記憶領域11に格納されていたパスワードDoP(1)~DoP(s)は、APがハイレベルでP2がロウレベルの場合に限り、OEB0に同期してパスワードラッチ回路521にラッチされる。ラッチされたDoP(1)~DoP(s)はDoPL(1)~DoPL(s)としてパスワードアクセス判定回路522に送られ、入力データDi(1)~Di(s)と比較される。これが一致していた場合、信号P2がハイレベルとなりアクセス制限が解除される。一方、パスワードライトデータ生成回路523は、記憶領域11への再書き込みデータDiP(1)~DiP(s)を生成する。

【0052】図9は、パスワードアクセス許可手順を示すタイミング図である。パスワードアクセス許可手順はDRAMで良く知られたリード・モディファイ・ライトのコマンドにより行なわれる。RASBロー遷移のタイミングでXアドレスが取り込まれ、CASBロー遷移のタイミングでYアドレスを取り込むと共にWEBをハイレベルとしてリード動作を指定する。所定のタイミングでOEBをローレベルにするとDoP(1)~DoP(s)が回路521にラッチされる。次にモディファイ・ライトに対応してWEBをロウレベルに遷移させ、Di(1)~Di(s)を与える。DoP(1)~DoP(s)とDi(1)~Di(s)とが一致していれば、P2はハイレベルとなるが、P2ハイ遷移はRASBハイ遷移に同期して行なわれるようにしている。これは、回路523から出力されたDiP(1)~DiP(s)の記憶領域11への再書き込みが終了した後にアクセス制限解除とするためである。特に以下の例では、“0”を再書き込みし、不正アクセスの再試行ができないようにしているので、この“0”再書き込みが確実に行なわれる必要がある。なお、RASBを規定外に早くハイ遷移させ、再書き込みを不成功に終わらせる試みがなされるかもしれない。そこで、後の図11に示すように、上記P2のハイ遷移は、ワード線活性化を制御するXL(図1の回路40で生成)に呼応するようにし、かつRASBが規定外に早くハイ遷移されても、XLを含む内部信号が再書き込み終了まで再書き込み状態を保持するような機能を付加しておく。ここでの説明に係る不揮発性メモリ装置は、DRAMと共通のコマンドを用いているので、ユーザにとって扱いやすく、また、回路構成も簡単にできる効果がある。

【0053】図10はパスワードライトデータ生成回路523の具体的な回路例である。P2がロウレベルの場合再書き込みデータDiP(1)~DiP(s)はすべて0となる。P2がハイレベルの場合再書き込みデータDiP(1)~DiP(s)



はDi(1)～Di(s)に一致する。このパスワード・ライトデータ生成回路の例によれば、不正アクセス時にはパスワードが"0 0"に書き換えられるので、"0 0"の場合にはアクセス制限を解除できないようにパスワードアクセス判定回路522の論理を構成することにより、不正アクセスの試行を重ねることができなくなり、高いセキュリティが得られる。なお、図9に示すようにRASBハイ遷移後にP2がハイレベルとなるように構成すると、Di(1)～Di(s)が正しく与えられた場合にもパスワードが"0 0"に書き換えられることになる。したがって、P2ハイ遷移の後、所望のパスワードを再書き込みする必要がある。あるいは、後の図11の信号P2Aのように、Di(1)～Di(s)が正しく与えられた場合直ちにハイ遷移する信号をP2のかわりに用い、P2ハイ遷移の後のパスワード再書き込みを不要にすることもできる。

【0054】図11はパスワードアクセス判定回路522の具体的回路例を示すものである。電源投入直後には、抵抗R521によりフリップフロップ回路の出力P2Aはロウレベルであり、高抵抗R522によりP2はロウレベルとなっている。パスワードアクセス解除手段が行なわれた場合、回路525-i (i = 1～s) はラッチされたパスワードDoPL(i)が入力データDi(i)に一致し、かつ0でない場合、ハイレベルを出力する。信号ZRBはDoP(1)～DoP(s)が全てロウレベルの場合に限りロウレベルとなる信号である。回路525-i (i = 1～s) の出力がすべてハイレベルであった場合、フリップフロップ回路の出力P2Aが反転し、さらにRASBハイ遷移に対応してXLが立ち下がったタイミングでP2がロウレベルからハイレベルに遷移する。

【0055】図12はパスワードラッチ回路521の具体的回路例を示すものである。P2がロウレベルでAPがハイレベルのときにOEB0がロウレベルに遷移すると、ラッチパルスLSが発生する。そして、DoP(1)～DoP(s)がDoPL(1)～DoPL(s)としてラッチされる。図12の遅延要素delayで定まる遅延時間の後、LSは再びロウレベルとなり、DoPL(1)～DoPL(s)はすべて0となる。上記遅延要素delayは、Di(i)が回路522に到達した後にLSがロウレベルになるようにその遅延時間が設定される。

【0056】図13は図11に用いられる信号ZRBを発生するパスワードオールゼロ認識回路であり、DoPL(1)～DoPL(s)のオア論理を出力とする。

【0057】以上図8から図13に示した具体例によれば、図1の説明における効果、特に項目(2)から

(5)の効果をえられることが明らかになる。

【0058】《不揮発性メモリ装置のその他回路の具体例》以下図14から図19に、図1における回路のその他の具体例を示す。

【0059】図14はライトデータ選択回路25の具体的回路例である。WEB0がロウレベルでライト動作の場合、APがハイレベル(記憶領域11の選択)ならDiP(1)

～DiP(s)が、APがロウレベルならDi(1)～Di(s)が、書き込みデータDiW(1)～DiW(s)としてデータバス26に送られる。

【0060】図15は出力先選択回路22の具体的回路例である。メインアンプ21からの読出しデータDoR(1)～DoR(s)は、APがハイレベルなら回路52にDoP(1)～DoP(s)として送られ、APがロウレベルなら回路23にDo(1)～Do(s)として送られる。

【0061】図16はアクセス許可回路50の具体的回路例である。ヒューズF50が接続状態では、オア回路の入力F50はハイレベルであり、信号P0はハイレベルである。すなわち、アクセス制限は解除されている。この状態で、最初に記憶領域11の初期パスワードを"0 0"以外に書き込んでおく。その後、ヒューズ切断用パッドに電圧を印加し、ヒューズF50を切断して、F50を高抵抗R50の働きによりロウレベルにする。これで本発明のメモリの初期設定が終了する。ヒューズ切断後は、P1あるいはP2の何れかがハイレベルとなった場合にP0がハイレベルとなり、アクセス制限が解除される。

【0062】図17はパスワードアクセスフラグAPの発生回路例である。記憶領域11のXアドレスを"11 1"に設定した場合、AX(1)～AX(n)のAND論理によりAPが生成される。

【0063】図18はリードアクセスに制限を設けたい場合に設けられるOEB0発生回路の具体的回路例である。APがハイレベルか、P0がハイレベルの場合には、内部アウトプットイネーブル信号OEB0は外部から与えられるアウトプットイネーブル信号OEBに一致する。すなわち、アクセス制限が解除される。AP、P0がともにロウレベルの場合には、OEB0はOEBによらずハイレベルとなり、リードアクセスは禁止される。

【0064】図19はライトアクセスに制限を設けたい場合に設けられるWEB0発生回路の具体的回路例である。図18に比べて回路190が加わっているが、これはDRAMで知られたアーリーライトコマンドを、P0がロウレベルの場合に記憶領域11に対して禁止するためである。回路190は後の図20に示すパスワード書き戻し方式をライトデータ生成回路523に採用する場合に必要となる。回路190において、RASBロー遷移から一定遅延後にOEBがロー遷移した場合に限り、S入力にセットパルスが与えられて出力Qがハイ遷移する。RASBがハイレベルに戻ると、R入力にリセットパルスが与えられて出力Qがロウ遷移する。P0がロウレベルでAPがハイレベルの場合、回路190の働きによりパスワードの読出しが行なわれていた場合に限り、メモリ内部のライトイネーブル信号WEB0は外部から与えられるライトイネーブル信号WEBに一致する。すなわち、ライトアクセス制限を受けない。ただし、この場合、図1に示すようにライトデータは外部信号DQ(1)～DQ(s)ではなく、パスワードアクセス

許可回路52で生成されたデータDiP(1)～DiP(s)となるので、アクセス制限を解除しない状態でパスワードが任意の値に書き換えられてしまう心配はない。P0がハイレベルの場合にも、当然WEB0はWEBに一致する。AP、P0がともにロウレベルの場合には、WEB0はWEBによらずハイレベルとなり、ライトアクセスは禁止される。

【0065】《パスワード ライトデータ生成回路の別の例》図20は、パスワード ライトデータ生成回路523の別の回路例を示すものである。図20においては、パスワードアクセス許可手段を行使した際、読み出され、回路521にラッチされたパスワードデータDoPL(1)～DoPL(s)の一部、たとえばDoPL(1)が0であった場合には0が書き戻され、1であった場合にはDoPL(1)～DoPL(s)が再書き込みされる。図10においては、必ず0を再書き込みするように回路523を構成していた。図10の場合、不正アクセスに対するセキュリティが極めて高い反面、不正アクセスが試みられた場合、あるいは解除手段として誤った入力データDi(1)～Di(s)を与えてしまった場合、パスワードアクセス制限解除手段が不能となってしまう。後者に対しては、パスワードを複数個、記憶領域11に格納しておけば対処できるが、いずれにせよ永続的アクセス制限解除手段の行使はなるべく避けたい場合がある。図20の回路523によれば、パスワードの一部のデータを、たとえばDoPL(1)が1になるように設定しておけば、同じパスワードが再書き込みされ、0になるように設定しておけばパスワードが自動消去される。ユーザは、メモリ内のデータ保護をある程度行いたい、制限解除が困難になるのは避けたい場合はDoPL(1)を1に設定し、たとえ制限解除が困難になってもデータ保護を確実に行いたい場合はDoPL(1)を0に設定するという様に、データ保護のレベルを選択できる。

【0066】《パスワード ライトデータ生成回路の更に別の例》図23は、パスワード ライトデータ生成回路523の更に別の回路例を示すものである。図23においては、図16の回路50による初期パスワード設定時には、FS50がハイレベルであり、パスワードデータの一部、たとえばDiP(1)は1となるように書き込まれる。その後、パスワードアクセス許可手段を行使した際、読み出されて、回路521にラッチされたパスワードデータDoPL(1)～DoPL(s)が入力データに一致しP2Aがハイレベルになった場合に限り、たとえばDoPL(1)は1に書き戻される。そうでなければDoPL(1)は0に書き戻され二度と1に戻らない。DoPL(2)～DoPL(s)はそのまま再書き込みされる。ここで、P2Aは一致検出時に直ちにハイレベルとなる信号であり、P2はパスワードデータ書き込み終了後にハイレベルとなる信号である。DoPL(1)が0だった場合、なんらかの不正アクセスが過去に試行されたと認識できる。

【0067】《WEB0発生回路の別の例》図21は、パスワードアクセス許可方式において用いられるWEB0発生回

路の回路例を示すものである。図19のWEB0発生回路を設けた場合、パスワードを知らない一般ユーザは、常にライトアクセスが禁止されていた。図21においては、メモリセルアレイ10の一部領域に記憶されたライトアクセスフラグに基づき、一般ユーザに対してライトアクセスを制限したり開放したりできる。その方法を要約すれば、電源投入時にはリード及びライトアクセス共に禁止されているが、一般ユーザは既知のメモリアドレスを指定することにより、該メモリ情報に依ってはリードまたはライトまたは両方の制限が解除されるというものである。WEB0発生回路についても同様なので、以下図21によりWEB0発生回路につき説明する。電源投入直後には、抵抗R40の働きにより回路401の出力はロウレベルとなっている。この状態では、図19と同様である。ただし、簡単のために図19の回路190に相当する機能は省略している。パスワード等によるアクセス制限解除手段を知っており、他のユーザに対してライトアクセスのみ開放し、リードアクセスを禁止したいユーザは、上記ライトアクセスフラグを、たとえばXアドレス"01 1"で指定されるメモリ領域の一部に"1"として格納しておく。ライトアクセスを行いたい一般ユーザは、該ライトアクセスフラグのX及びYアドレスを指定した読出し動作を行う。すると、該ライトアクセスフラグはたとえばDo(1)として読み出される。ここで、まだすべてのアクセスは禁止されているため、Do(1)は外部信号DQ(1)としては出力されないが、回路22からは出力される。これを図21の回路401に入力すると、Do(1)が"1"に設定されていた場合、ライトアクセス制限が解除される。なぜなら、ライトアクセスフラグのXアドレス入力により信号APEがハイレベルとなり、アンド回路の働きにより回路401のフリップフロップが反転して出力がハイレベルに変化するからである。この結果、外部信号WEBは内部信号WEB0に常に一致するようになる。ただし、ライトアクセスフラグ自体を勝手に書き換えられると困るので、APEがハイレベルの場合、回路401の出力が機能しない構成にしている。一般ユーザに対してライトアクセスを禁止したい場合は、ライトアクセスフラグを"0"に設定しておけばよい。パスワード等によるアクセス制御解除手段を知っているユーザはP0をハイレベルにしてライトアクセスフラグを書き換えることができる。以上はライトアクセスに関して述べたが、リードアクセスに関しても同様である。すなわち、ライトアクセスフラグと同じアドレスで指定され、たとえばDo(2)として読み出される情報を、リードアクセスフラグとしてWEB0発生回路を構成すればよい。

【0068】上記によれば、パスワードを知っているユーザは、これを知らない一般ユーザに対して、本発明の不揮発性メモリ装置へのライトアクセス／リードアクセスを任意に開放したり、禁止したりできる。この結果、後述の応用例にも示すように応用範囲の広いセキュリティ

ィ機能つき汎用不揮発性メモリ装置が得られる。

【0069】《パスワードアクセス判定回路の別の例》  
図20の回路523において、設定によっては常に同じパスワードが再書き込みされる例を示した。この場合、不正アクセスを試みるものは、考えられるあらゆるパスワードを入力してみるであろう。この試行はコンピュータのプログラムにより比較的高速に行うことができる。図22は、このような不正アクセスを困難にするパスワードアクセス判定回路522の回路例である。図22の回路522においては、一つのパスワード入力によりアクセス制限解除に失敗した場合、電源を再投入しなければ再試行ができない。回路522において、電源投入時には抵抗R521の働きにより、フリップフロップ回路の出力P2Bはハイレベルとなっている。しかし、図11に示すパスワードラッチ回路のラッチ信号LSはロウレベルであるので、高抵抗R522の働きによりP2はロウレベルである。パスワードアクセス許可手段が行使されると、内部パスワードDoPL(1)～DoPL(s)が入力パスワードDi(1)～Di(s)に一致していなかった場合、あるいはDoPL(1)～DoPL(s)が“0”であった場合、回路522のラッチ出力P2AがLSから遅延要素delay(521)で規定される時間だけ遅延したタイミングで反転しロウレベルとなる。したがって、さらに遅延要素delay(522)で規定される時間だけ遅延したタイミングでP2がハイレベルになるのは、P2Aがハイレベルに維持されていた場合、すなわち内部パスワードDoPL(1)～DoPL(s)が入力パスワードDi(1)～Di(s)に一致し、かつ“0”でなかった場合だけである。続けて他の入力パスワードでパスワードアクセス許可手段を行使しても、もはやP2BすなわちP2を反転させることはできない。電源を再投入しなければならぬ。本発明の実施例によれば、不正アクセス失敗時に内部パスワードを自動消去しない方式においても、不正アクセスを試行錯誤する手間が増えるのでセキュリティを高めることができる。

【0070】以上本発明の構成とその具体的な回路例を述べてきた。以下では本発明の不揮発性メモリ装置の応用例を述べる。以下の応用例は、図1のチップ形態の不揮発性メモリ装置（即ち半導体不揮発性メモリ）を実装したICメモリカード形態での応用を想定する。

【0071】《応用例1》セキュリティ機能を有した汎用ICメモリカードとして個人データの保管に用いることができる。上記パスワードの書き込みは、個人データを書き込む本人が、ICメモリカード発行時の初期パスワードを変更して行う。不揮発性メモリ装置内のパスワードがリテンション不良等により失われるか、パスワードアクセス許可回路が故障して、パスワードアクセス許可手段によるアクセス制限解除が不能となった場合、永続的アクセス許可手段によりアクセス制限を解除する。

【0072】なお、パスワードアクセス許可手段が機能しなくなる場合として、第三者が不正なアクセスを試み

た場合も考えられる。許可手段の行使により、内部パスワードが自動消去されるからである。したがって、永続的アクセス許可手段の存在、あるいはその詳細な手順は、ICメーカなどの権威ある機関のみが知っているようにするのがよい。ICカードの保有者はたとえばICメーカにデータの修復を依頼し、ICメーカは永続的アクセス許可手段によりアクセス制限を解除する。ただし、この場合権威ある機関は、依頼者が確かにICメモリカードの所有者であることを確認する手段を持っている必要がある。ICカード表面に個人のサインを記せるようにしておいてもよい。

【0073】慎重なユーザは、ICメモリカードへのパスワード書き込みを、自宅のパソコンなど信用できる装置を用いて行うことが推奨される。公共の装置では、たとえばキーボードから入力したパスワードが装置内の記憶装置に別途保存されるように改変されているかもしれないからである。記憶領域11に複数のパスワードを書き込んでおき、公共の装置でICメモリカードのアクセス制限解除を行う際にパスワードを新たに書き込まないようにすれば（自動消去されたままに放置すれば）、少なくともあらかじめ書き込んだパスワードの数より一つ少ない回数だけ、公共の装置でICメモリカードを用いることができ、かつ高いセキュリティが維持される。最後の一つのパスワードは自宅のパソコンでパスワードを再書き込みする際に用いられる。

【0074】上述した図20、図23で説明したパスワード・ライトデータ生成手段により、第三者が不正なアクセスを試みた場合にもアクセス制限解除が不能とならない（パスワード自動消去を行わず再書き込みする）選択機能を設けてもよい。あるいは、上述したように、パスワードを知らないユーザに対して、ライトアクセスあるいはリードアクセスあるいはその両方を、任意に禁止／開放できる機能を付加すると便利である。

【0075】《応用例2》いわゆる“親展”に相当する機能が実現できる。Bは書面に代わりICメモリカードをAに郵送する。ICメモリカードを受け取ったAは、電話等でBにパスワードを聞き、パスワードアクセス許可手段によりICカードのアクセス制限を解除して内容を読み出す。アクセス制限解除に失敗した場合、不揮発性メモリ装置内のパスワードがリテンション不良等により失われたか、パスワードアクセス許可回路が故障したか、あるいは郵送中になんらかの不正アクセスがありパスワードが自動消去されたと判断できる。また、パスワードアクセス許可手段により正しくアクセス制限が解除された場合は、郵送中にデータが改ざんされた可能性はほとんどないと判断できる。

【0076】パスワードアクセス許可手段が不能となっており、B自身もデータを失うなど再郵送が不可能な場合、ICカードの保有者はたとえばICメーカにデータの修復を依頼し、ICメーカは永続的アクセス許可手段により

アクセス制限を解除する。

【0077】《応用例3》本人の認証に应用できる。遠隔地にいる者Aを通信により認証する必要がある場合、認証を与える者Bは、本発明のICカードにパスワードとこれとは別の認証用情報とを書き込んだ後、あらかじめAに手渡しておく。上記パスワード及び認証用情報はBのみ知っている。遠隔地にいるAを認証する場合、Bは通信手段を介してパスワードアクセス許可手段によりICカードのアクセス制限を解除する。ここで、パスワードアクセス許可手段はパスワードを知っているBのみが与えることができる。アクセス制限が解除されたら、Bは認証用情報を通信回線を介して読出し、これが、Bがあらかじめ設定した値に一致していれば、(ICカードがAから別人に手渡されていない限り)通信相手がAであると認証できる。さらに、不揮発性メモリ装置内のパスワードがリテンション不良などにより失われるか、パスワードアクセス許可回路が故障していた場合、Bは永続的アクセス許可手段を用いてアクセス制限を解除し、認証用情報を読み出すことができる。この場合は、通常電圧で永続的アクセス許可手段が行使できるように設計しておくほうが良い。

【0078】応用例3の変形例として、情報サービスがある。本発明のICメモリカードはプリペイドカード兼情報格納メモリとして機能する。情報サービスを受ける者Aは、情報サービスを提供する側Bからお金と引き換えに本発明のICカードを受け取る。Bはあらかじめ上記パスワード及び認証用情報をICカードに書き込んでおく。後に、通信回線を介してAが情報を要求したら、Bはパスワードアクセス許可手段により通信回線を介してICカードの認証用情報を読み出す。これがBがあらかじめ設定した値に一致していれば、ICカードに情報を書き込む。情報としては、たとえばゲームソフトなどがある。書き込み終了にあたって、たとえば上記《WEB0発生回路の別の例》の節で説明した手段にしたがって、ライトアクセスのみ禁止し、リードアクセスを開放するモードに設定しておく。Aは本発明のICカードをゲーム機に装着して使用する。

【0079】パスワードを金額に応じた数だけ書き込み、金額に応じた情報を得られるようにすることもできる。あるいは、ライトアクセスの禁止を所定ブロック領域に制限し、ライトアクセス可能なブロックを設けて、そこにゲームに関する個人情報を記録できるようにしてもよい。

【0080】不揮発性メモリ装置内のパスワードがリテンション不良などにより失われるか、パスワードアクセス許可回路が故障していた場合、Bは永続的アクセス許可手段を用いて情報サービスを行うことができる。

【0081】以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲にお

いて種々変更可能であることは言うまでもない。

【0082】例えば、メモリセルは強誘電体メモリセルに限定されず、EEPROM若しくはフラッシュメモリ用の不揮発性メモリセルなどであってもよい。不揮発性メモリ装置は半導体集積回路チップとして実現し、或いは当該チップを実装したICメモリカードとして実現できる。ICメモリカードの場合、当該メモリチップのセキュリティ向上のためにマイクロコンピュータのようなデータ処理半導体集積回路と一緒に実装することを要しない。本発明ではメモリ装置それ自体で必要なセキュリティを実現している。

【0083】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

【0084】通常使用されるパスワードアクセス許可手段が故障しても、あるいは記憶領域のパスワードがなんらかの障害、たとえば不揮発性メモリセルのリテンション不良やハードエラー、ユーザの設定パスワード忘却などにより失われても、永続的アクセス許可手段によりアクセス制限回路を解除できるので、高信頼のセキュリティ機能が得られる。

【0085】パスワードを書換可能な不揮発性メモリセルに格納するので、たとえば一回ごとにこれを変更することにより、入力パスワードとの直接比較による単純なアクセス制限解除方式を採用できる。更に、内部パスワードと入力パスワードの不一致時には、内部パスワードを自動消去するなど、試行錯誤による不正アクセスを防止する施策も施すことができる。このような単純なアクセス制限解除方式の採用によりチップ面積が低減でき、その結果コストを下げられる。したがって、特に汎用メモリチップおよび汎用ICカードに適したセキュリティ機能付き不揮発メモリが得られる。

【0086】パスワードを書換可能な不揮発性メモリセルに格納するので、パスワードを第三者に知られてもこれを変更することにより引き続きメモリのセキュリティを維持することができる。

【0087】不正アクセス時の内部パスワード消去を行えば、単純な構成で極めてセキュリティの高いメモリが得られるが、パスワードアクセス許可手段によるアクセス制限解除が不能となる。これに備えて、永続的アクセス許可手段を設け、非常時にもアクセス制限の解除が可能になっている。永続的アクセス許可手段を通常の使用条件の範囲外に設定しておけば、この存在を知らないユーザが意図せず該手段を行使する危険を回避でき、極めてセキュリティが高く、かつアクセス制限解除が不能となる危険性も小さい汎用のメモリが得られる。

【0088】不正アクセス時の内部パスワード消去を行えば、ユーザはパスワードアクセス手段が不能となったことにより不正アクセスが試みられたかも知れないと察

知できる。これによりユーザはセキュリティ態勢をより強化するなどの対策をとることができる。

【図面の簡単な説明】

【図 1】本発明の不揮発性メモリ装置の一例を示すブロック図である。

【図 2】永続的アクセス許可回路の一例を示すブロック図である。

【図 3】ヒューズ状態信号発生回路の一例を示す論理回路図である。

【図 4】ヒューズ状態論理回路の一例を示す論理回路図である。

【図 5】ヒューズ切断モード発生回路の一例を示す論理回路図である。

【図 6】ヒューズ切断アドレス発生タイミング図である。

【図 7】一回のみ起動するヒューズ切断モード発生回路の一例を示す論理回路図である。

【図 8】パスワードアクセス許可回路の一例を示すブロック図である。

【図 9】パスワードアクセス許可信号発生タイミング図である。

【図 10】パスワード・ライトデータ生成回路の一例を示す論理回路図である。

【図 11】パスワードアクセス判定回路の一例を示す論理回路図である。

【図 12】パスワードラッチ回路の一例を示す論理回路図である。

【図 13】パスワード・オールゼロ認識回路の一例を示す論理回路図である。

【図 14】ライトデータ選択回路の一例を示す回路図である。

【図 15】出力先選択回路の一例を示す回路図である。

【図 16】アクセス許可回路の一例を示す論理回路図である。

【図 17】パスワードアクセスフラグ発生回路の一例を示す論理回路図である。

【図 18】WEB0発生回路の一例を示す論理回路図である。

【図 19】OEB0発生回路の一例を示す論理回路図である。

【図 20】パスワード・ライトデータ生成回路の一例を示す論理回路図である。

【図 21】WEB0発生回路の一例を示す論理回路図である。

【図 22】パスワードアクセス判定回路の一例を示す論理回路図である。

【図 23】パスワード・ライトデータ生成回路の一例を示す論理回路図である。

【符号の説明】

A(1)～A(n) 外部アドレス信号

DQ(1)～DQ(s) 外部データ信号

RASB ラス アドレス ストロープ バー信号

CASB カラム アドレス ストロープ バー信号

WEB ライト イネーブル バー信号

OEB アウトプット イネーブル バー信号

WEB0 内部ライト イネーブル バー信号

OEB0 内部アウトプット イネーブル バー信号

AX(1)～AX(n) Xアドレス信号

AY(1)～AY(n) Yアドレス信号

AZ(1)～AZ(n) ヒューズ切断アドレス信号

Di(1)～Di(s) 内部書き込みデータ

Do(1)～Do(s) 内部読出しデータ

DiP(1)～DiP(s) パスワード書き込みデータ

DoP(1)～DoP(s) パスワード読出しデータ

P0 アクセス許可信号

P1 永続的アクセス許可信号

P2 パスワードアクセス許可信号

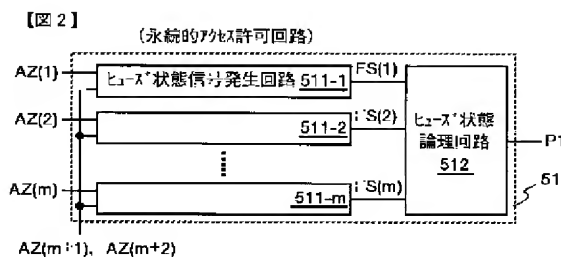
XL Xアドレスタイミング信号

YL Yアドレスタイミング信号

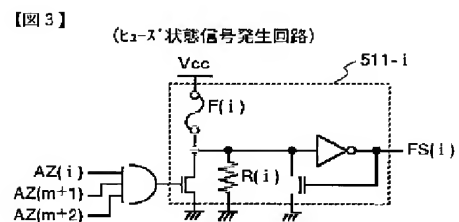
SP ヒューズ切断アドレスタイミング信号

AP パスワードアクセスフラグ

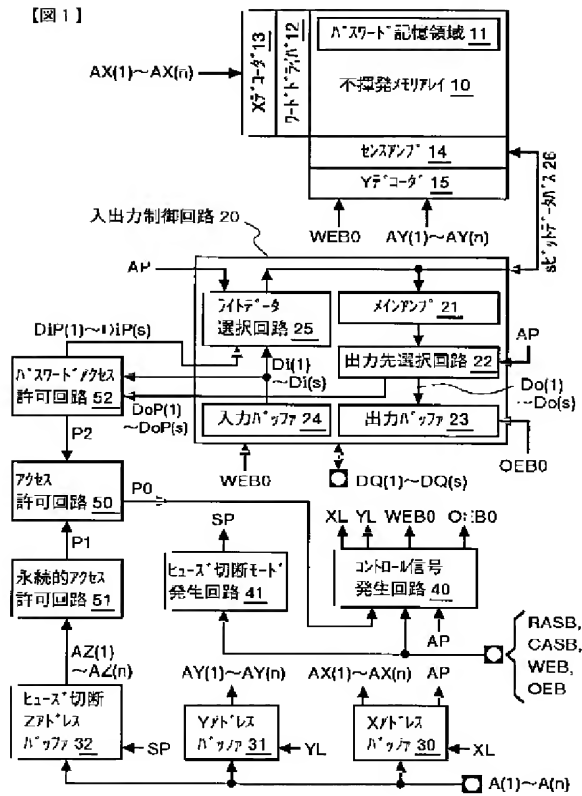
【図 2】



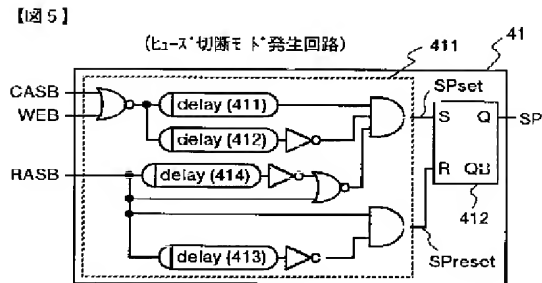
【図 3】



【図 1】

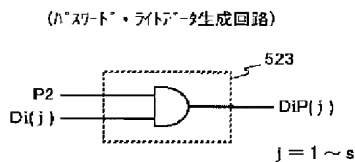


【図 5】

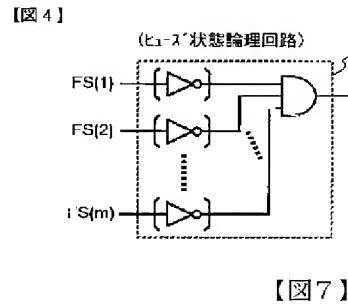


【図 10】

【図 10】

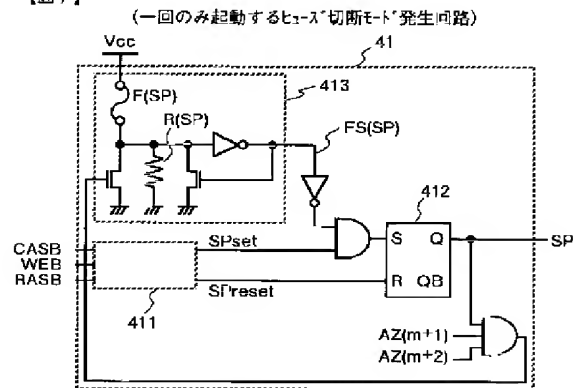


【図 4】



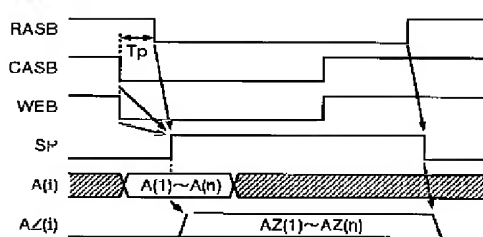
【図 7】

【図 7】



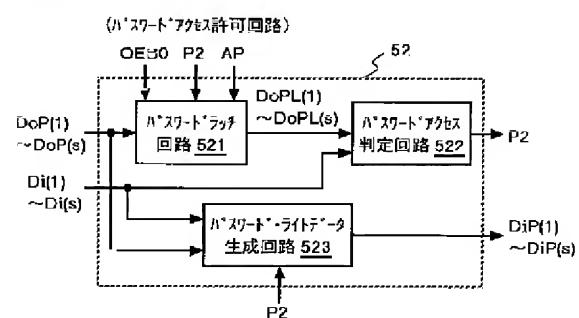
【図 6】

【図 6】



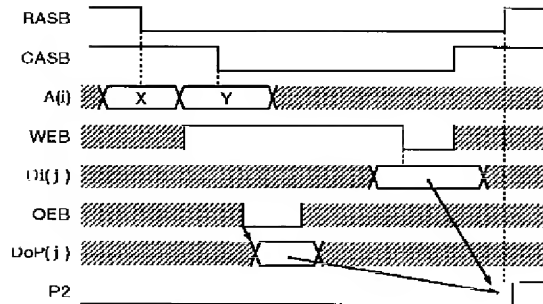
【図 8】

【図 8】



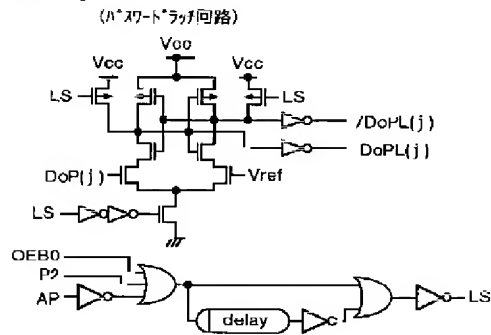
【図 9】

【図 9】



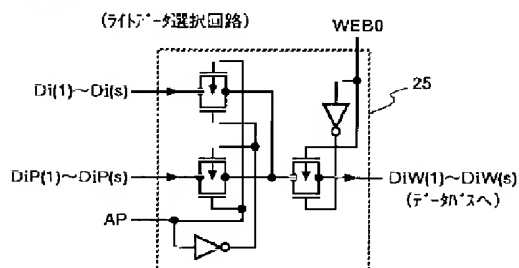
【図 12】

【図 12】



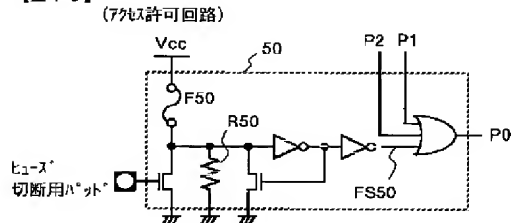
【図 14】

【図 14】



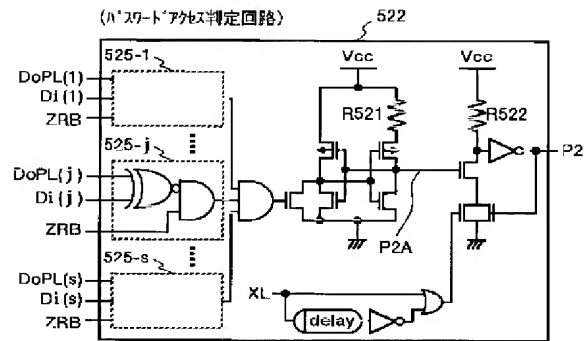
【図 16】

【図 16】



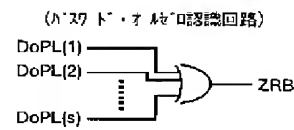
【図 11】

【図 11】



【図 13】

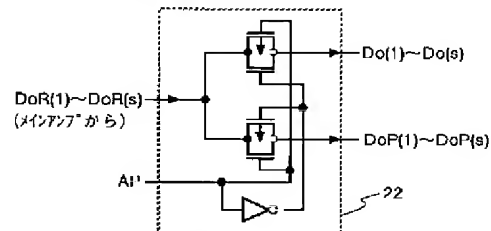
【図 13】



【図 15】

【図 15】

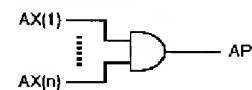
(出力先選択回路)



【図 17】

【図 17】

(n'スタート'アクセス'発生回路) ...X7'ト'ス "11...1" の場合...

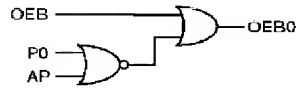




【図18】

【図18】

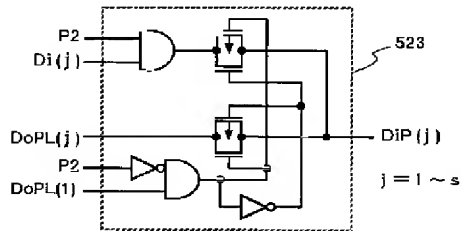
(OEB0発生回路)・・・リトアクセス禁止の場合・・・



【図20】

【図20】

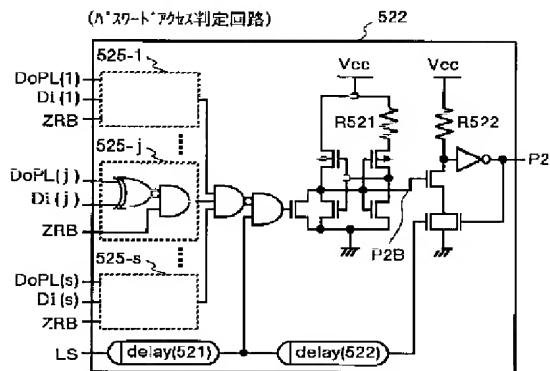
(A\*スタート・ライト・タ生成回路)



【図22】

【図22】

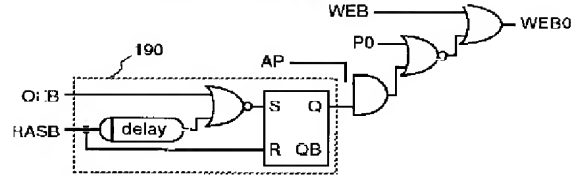
(A\*スタートアクセス判定回路)



【図19】

【図19】

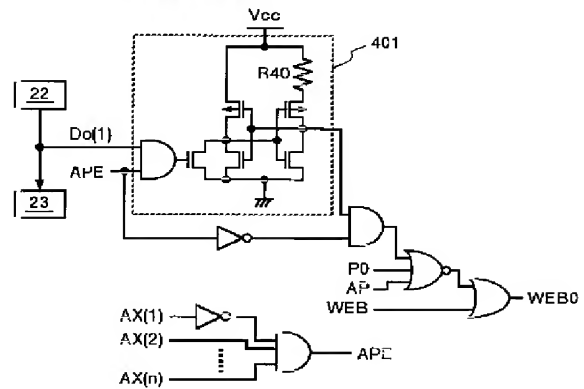
(WEB0発生回路)・・・ライトアクセス禁止の場合・・・



【図21】

【図21】

(ライトアクセス制限設定回路)



【図23】

【図23】

(A\*スタート・ライト・タ生成回路)

